HIT Standards Committee
Final Summary
Summary of the February 24, 2010, Meeting

KEY TOPICS

1. Call to Order

Judy Sparrow, Office of the National Coordinator (ONC), welcomed participants to this meeting of the HIT Standards Committee, and conducted roll call.

2. Opening Remarks From the National Coordinator

David Blumenthal, National Coordinator for Health Information Technology, opened the meeting by welcoming Committee members and thanking them for their efforts. He expressed enthusiasm for hearing input from the Committee on the Interim Final Rule (IFR). In the coming weeks, Committee members will be updated regarding programs designed to support the provider and patient communities to make the best meaningful use of health information technology and build on the standards and certification criteria that the Health Information Technology Standards Committee (HITSC) has helped establish. The ONC is hard at work on the Notice of Proposed Rulemaking (NPRM), which should be released in the near future.

3. Overview of the Meeting

Jonathan Perlin, HITSC Chair, also welcomed Committee members and expressed appreciation for their input, as well as that of the public, in helping to move HITSC activities forward. These open, ongoing dialogs are extremely helpful in obtaining the best input from a broad cross-section of experts. He also thanked members of the HITSC workgroups, who have been synthesizing this input and incorporating it into their respective areas. He noted that this HITSC meeting would feature reports by the Chairs of the Clinical Operations, Clinical Quality, Privacy and Security, and Implementation Workgroups.

John Halamka, HITSC Vice Chair, added that Committee discussions would focus on the IFR and characterized it as an evolving document in that the Committee will be providing continuous guidance and refinement. He noted that there is likely to be a continuous tension (and necessary decision making) related to the level of specificity in the IFR. In the next 6 months, ONC is expected to develop and release Requests for Proposals (RFPs) related to the standards process (ONC issued an RFP on standards harmonization a few days before this Committee meeting).

> **Action Item #1:** Minutes from the last HITSC meeting, held on January 20, 2010, were approved by consensus.

4. Clinical Operations Workgroup: Comments and Discussion on the IFR on Initial Set of Standards, Implementation Specifications, and Certification Criteria for EHRs

Jamie Ferguson and John Halamka led this presentation. A public hearing of the Clinical Operations Workgroup's Vocabulary Task Force was held on the day prior to this meeting. The subject was rules for governing the subsets and value sets of the adopted vocabularies needed by implementers of electronic health records (EHR) technology. Three panels were held, one comprised of EHR vendors, one of terminology service providers, and one of content exchange standards development organizations. This work will continue through March. Materials will be made available online, and an update may be presented at the next HITSC meeting.

The Clinical Operations Workgroup has finalized a recommendation to broaden the adopted standards for content exchange to families of standards. Implementation guidance changes less frequently than the releases of the underlying base standard—this issue can be addressed by broadening the adopted standards in the IFR and providing implementation guidance through alternative mechanisms such as advisory letters, guidance letters, and circulars, as well as in the testing and certification program, rather than in the IFR itself. Specifically, the Workgroup recommends that the families of standards should include the National Council for Prescription Drug Programs (NCPDP) SCRIPT family, the HL7 version 2 family, the HL7 Clinical Document Architecture family, and others. Implementation guidance would have to be provided by the alternative mechanisms at the same time that the final rule is promulgated. Regulation is hard to change; the declaration of broad families of standards, with implementation guidance that can evolve separate from the regulation, would avoid the problem of hampering progress.

The Workgroup also recommended considering minimum implementation guides in the final rule. Multiple implementation guides do not appear to be a problem, but a minimum requirement may be needed in the regulation. The intent is to set a floor, but without ossifying the technology. The Workgroup did not reach consensus on this point and solicited feedback from Committee members.

In terms of interoperability, Jamie Ferguson indicated that the Clinical Operations Workgroup is requesting clarification of what is required inside the EHR versus what is required only for interoperability at the borders. The Workgroup recommended that minimum vocabulary subset requirements for interfaces/interoperability should be mandated in certification and/or testing. These subsets would provide a floor that most implementers would have to exceed.

Different documents may be best for different purposes. It is not clear how to use CCR as a source for quality reporting. Also, in the NPRM, there is a note that claims attachments can use both CDA level 1/level 2 (which are human readable only) and CDA level 3 (which is machine readable). Level 2 implies no machine readability. The Clinical Operations Workgroup would support a recommendation to go the same way with CDA as with claim attachments (i.e., to allow level 3 as well).

With regard to vocabulary, the Workgroup recommended that convenience subsets and value subsets—including frequency-based convenience subsets ("starter sets") and quality measure value sets—should be published, but that medical specialty convenience subsets are a lower priority. Releases of adopted vocabulary standards should be coordinated in advance but need not occur on a precisely regular basis. Although the Workgroup is recommending the publication of convenience subsets, mechanisms should be provided for EHR users to easily

implement vocabulary beyond these subsets. The workgroup specifically recommended including: (1) the adoption of standards for vital signs, and (2) expanded vocabularies for medication allergies. Two specific potential inconsistencies in requirements were also discussed, but no specific resolutions were recommended. Jodi Daniel clarified that because the IFR is a regulation, it would supersede any previous inconsistencies published in guidance.

The following comments were made in discussion:

- Carol Diamond commented that the Committee's recommendations should be guided by the framing principles developed in the implementation hearing, including the principle that implementation guides should be human readable, testing should be available, and there should be an open-source implementation reference if possible.

- Christopher Chute suggested that the framework that the Workgroup was proposing needs to be balanced by a shared goal of maintaining the practical nature of interoperability. The Committee cannot compromise the goal of interoperability with underspecified recommendations.

- Stanley Huff voiced support for the concept of greater flexibility but expressed concerns similar to those of Christopher Chute. If flexibility in versions of standards is allowed, what does that imply in terms of certification or other kinds of conformance testing? How can conformance be done, and how can there be an exact target at a particular point in time, while simultaneously allowing flexibility? It was noted that the Workgroup is seeking alternative mechanisms for getting those exact targets within a framework that allows advancement. An example involving Medicare Part D, which requires the use of a version that has been superseded by newer ones, was mentioned. Concerns were also raised about possible conflicts with the Medicare Modernization Act (MMA), which is very specific about versions to be used.

- In response to a question, Jodi Daniel explained that there are limitations on what can be adopted and how much flexibility can be allowed without obtaining comment on later versions of the IFR. The question of how much can be done through guidance rather than through the statute would need to be clarified by the General Counsel's office. Specificity as to a version number that is a floor might be acceptable.

- David Blumenthal pointed out that a potential problem with relying on guidance is that it circumvents the rigorous processes of rulemaking that allow for all interested parties to comment before changes are made. Jonathan Perlin commented that it is challenging to develop a set of specifications that is sufficiently specific so as not to be viewed as arbitrary and capricious but is also forward compatible to allow for future functionalities.

- Wes Rishel commented that writing a specification that includes options can compromise interoperability and scalability. Certification should be precise, but the emphasis in implementation should be on "getting the job done." Adapting standards to a use case while still having standards supported by a regulatory process is the only way to deal with the need for continuous updating. Interoperability is not possible without a very specific and detailed

specification. He suggested using very specific, fairly rapidly evolving standards for certification, with a public process for achieving consensus that is shorter than the regulatory process but nevertheless public. However, this should not be translated into an imperative for a hospital to use that standard to get the job done. Hospitals should not be required to change something that is working well.

- It was noted that some process must be identified for allowing standards to evolve and adapt, but this must be decoupled from the way that hospitals and practices achieve their business goals.

- John Klimek commented that the NCPDP considers the term "version" to means that there is some additional functionality in a newer version that meets an industry need. There are costs associated with moving to a new version, however, and therefore there are concerns about a law requiring its use. Losing interoperability also is an important concern; the pharmacy world depends on interoperability.

- Janet Corrigan explained that in the short term, it is a good idea to include a floor and some degree of flexibility in the regulations. In the long term, however, there are inherent problems with this approach because the field can move rapidly. It is difficult if not impossible to obtain comparable data if people are using different standards. There is a need to focus particular attention on the ongoing process for promulgating standards and for raising the floor and deciding how much flexibility to allow. It might be worthwhile to consider exploring quasi-regulatory processes for promulgating standards that the government can accept, such as the use of private-sector standard-setting organizations.

- Chris Ross cautioned that it likely is not possible to leap to codification in one jump. He also cautioned that the regulatory framework needs to be adaptable to new developments and inventions. He also asked how HL7 will respond to the goal of setting a floor of standards and expressed support for Janet Corrigan's concept of using private-sector standard-setting organizations. Kevin Hutchinson noted that pharmacies and EHRs are at different levels, but this is not causing conflict in allowing transactions to flow. The existence of multiple levels is allowed for a period of time, after which a notice is issued indicating that the network is being moved to a certain minimum standard.

- David McCallie noted that the regulation should define interoperability rather than specifying the standard to be used to achieve it.

- Cita Furlani expressed support for the concept of applying private-sector-developed standards and the idea of defining the result rather than the process.

- Jodi Daniel said that it was her impression that the group was supporting flexibility, but that the question was how to accomplish it. She asked whether there could be difficulties if a floor is set and then a version comes out that has significant changes that create interoperability problems. Complete backward compatibility may not always be possible. A member of the Clinical Operations Workgroup said that this was the reason why complete consensus was not achieved on the recommendation to have minimum implementation

guidelines. Jodi Daniel further noted that the statute requires regulation and adoption of standards for regulation. Therefore, there are statutory limitations on what the Committee can do. There is some question as to whether the statute will allow acceptance of newer versions or requires specification of a particular version.

- Jodi Daniel said interactions with other regulatory standards, such as MMA standards and HIPAA standards, must be considered. The standards need to align with one another so that compliance with all of them is possible. She has already communicated with the Centers for Medicare and Medicaid Services (CMS) to try to obtain clarification.

- Dixie Baker observed that problems could arise when organizations try to get differently coded modules certified. Translators may not always be able to adequately deal with these situations. Wes Rishel explained that nothing in the process of certifying modules ensures that two modules can work together to meet the meaningful use requirement.

- Anne Castro made the distinction between certifying an EHR and certifying interoperability. These are two different activities that do not necessarily need to be combined. Standard interfaces need to be created and made available. This may represent an RFP opportunity for ONC. Jonathan Perlin commented that border management and interoperability between certified and noncertified elements of information systems constitute a central issue. Further guidance as to the exactness of the requirement is needed.

- Stanley Huff spoke in favor of requiring compliance with standards only at the borders, not within systems. If compliance is required within systems, there is a risk of being unable to record information that is needed for patient care or patient safety because a suitable code does not yet exist. Carol Diamond agreed that the Committee's focus should be only at the borders, not within organizations. She also noted that modules that do not communicate outside the borders may not need to be certified, and that it is impossible to certify all possible interactions between all modules.

- Christopher Chute noted that there was still confusion about the difference between meaningful use and certification. Certification of technology is not a measure of meaningful use. He agreed that interoperability should be required only at the borders.

- David Blumenthal explained that criteria only attest to the presence of a capability; they cannot ensure that the capability is used to its full extent or even to any extent. The motivation to use it comes from the incentives in the meaningful use incentive regulation. The requirements of interoperability will need to be laid out in the meaningful use NPRM. The rules and the certifiers cannot create meaningful users. He asked how specific the standards built into EHRs need to be to achieve the necessary interoperability.

- Jamie Ferguson said that the workgroup agreed that complete specificity is needed with regard to interoperability to allow achievement with the meaningful use objectives, but that the group was struggling with the question of how to achieve that specificity – through regulation or other means. Chris Ross said that he believed that different opinions were being expressed because the individuals expressing them have experience with different use

cases, and the use cases ultimately drive the level of specificity to which different entities must adhere. Without agreement on shared use cases, this disagreement will not go away.

- Jonathan Perlin summarized the discussion thus far by noting that there was consensus about the need for specificity sufficient for interoperability. The point made about different use cases determining the viewpoint that individuals have brought to these discussions is important. There is a consensus that standards should be applied only at the borders. No consensus has been reached, however, about how to achieve interoperability—additional efforts are needed in this regard.

- Carol Diamond asked for clarification on the process of developing a final Committee document. Jodi Daniel explained that the Co-Chairs of the workgroups will prepare a recommendation letter based on their own discussions and the discussions that take place at this meeting and that the Chair and Co-Chair of the HITSC will sign off on that letter and submit it to David Blumenthal. It was agreed that workgroup members would have an opportunity to review the recommendation letters before they are submitted.

- Dixie Baker asked that the report from this meeting capture that the model of certifying EHR modules does not support the concept of certifying at the borders only. It was then clarified that certification is related to meaningful use, which can be internal. This does not necessarily imply that the module is certified for interoperability.

- Wes Rishel expressed the view that it is necessary to find a way to let discovery happen without it instantly becoming a regulation. The principles that were adopted by the Implementation Workgroup include adopting things after they have been proven in industry. An approach for indicating that meaningful use requirements may be ahead of the standards in some areas is needed.

- Jim Walker emphasized the need to clearly communicate the narrow definition of certification (i.e., that it does not necessarily imply interoperability) to the market.

Action Item #2: The report of the Clinical Operations Workgroup was accepted by consensus.

5. Clinical Quality Workgroup: Comments and Discussion on the NPRM and IFR

Janet Corrigan explained that during a recent conference call, Clinical Quality Workgroup members reviewed: (1) quality measures listed within the NPRM with respect to those recommended by the HITSC, and (2) the adequacy of IFR standards to support the requirements of measures in the NPRM. There are 90 ambulatory measures and 40 hospital measures in the NPRM; the list of measures includes 15 of the 17 measures recommended by the HITSC. The two measures recommended by HITSC but not included in the NPRM are medication reconciliation (NQF #0097) and the ability for providers with HIT to receive laboratory data electronically directly into their qualified/certified EHR system as discrete searchable data elements. These measures were replaced by metrics for EHR reporting for the reporting of

exchange of clinical information, medication reconciliation, and summary of care records, among others.

Specialties were addressed by the list of core measures in the NPRM, with three core measures that apply to all specialties. In the case of primary care, there is a large number of measures (29) compared with specialties such as cardiology (10 measures), oncology (6 measures), neurology (5 measures), etc. Janet Corrigan commented that there is a need to consider the burden associated with this volume of measures should they all move forward. She also noted that the Workgroup did not attempt to go back and comment on whether the many new measures that were put forward are appropriate and the best measures for meaningful use; this falls within the purview of the HIT Policy Committee.

Floyd Eisenberg explained that the Workgroup has concerns associated with the IFR in three main areas. With regard to a medication allergy list, there are no standards specified in 2011. UNII codes are listed as a candidate stage 2 vocabulary—UNII describes allergies at the drug component level and not at the drug level. The Clinical Operations Workgroup specifically suggested allergies at the drug level; the component level is problematic for the near or mid-term, if not the long term. *The Workgroup recommended that a medication allergy standard be required for measurement in 2011 at the drug level, not the component level.*

Another area of concern noted by the Workgroup relates to vital signs. No standard was suggested for stage 1; CDA template is a candidate for stage 2, but depending on what level of CDA is used, it would need to be a level that specified detail and not just a human readable component under "vital sign." A vocabulary for vital signs (especially blood pressure) and findings (e.g., body mass index) is therefore needed to compute the measures in a standard manner. *The Workgroup recommends that a vocabulary standard for vital signs and clinical findings is required for quality measurement in 2011. LOINC or SNOMED codes have been suggested in prior work of the HITSC* (implementing both would pose a significant challenge; it would be helpful to have a harmonized decision on which standard is to be used).

The third area of concern identified by the Workgroup is unites of measure—no units of measure were indicated in stage 1 (UCUM is a candidate standard for stage 2). Floyd Eisenberg explained that standard units of measure are required to consistently calculate measures that require laboratory results, medication dosages, vital signs, and observations. *The Clinical Quality Workgroup is recommending that units of measure standards are required to consistently calculate quality measures for stage 1—UCUM has been suggested previously by HITSC and will add value.*

In discussion, the following points were made:

- One Committee member asked, given concerns about the generality of specifying CDA and issues surrounding CCR, if CC32 were adopted, would that over specify, underspecify, or be "just right?" Floyd Eisenberg explained that it would resolve the specificity issues; there are elements within CC32 that may not be necessary for the measures.

- Floyd Eisenberg was asked whether PQRI was required in stage 1, and clarified that the second component for stage 2 was that other standards may be recommended in the future. The Workgroup's recommendation does not remove this. It would be problematic to temporarily ask implementers to go in one direction and then change.

Action Item #3: Committee members accepted the recommendations of the Clinical Quality Workgroup by consensus.

6. Privacy and Security Workgroup: Comments and Discussion on the IFR

Dixie Baker noted that Privacy and Security Workgroup members were asked to respond to a series of questions regarding the IFR, relative to: (1) the overall EHR technology certification approach; (2) reasonableness, sufficiency, and specificity of certification criteria; (3) reasonableness and sufficiency of adopted standards; (4) solicitation for comments regarding the omission of domain name service, directory service, and consistent time; (5) reasonableness and technical feasibility of the accounting of the disclosures standard; and (6) perceived gaps. Dixie Baker and Steve Findlay reviewed a number of concerns and recommendations identified by the Workgroup in the following areas:

- Example Standards: Specification of functional standards with no examples provided in the body of the IFR creates uncertainty and risk for both developers and certifiers. The Workgroup supports the overall approach, which provides flexibility and allows for innovation, but there is concern that it may not provide sufficient specificity for EHR developers and certifiers. *The Workgroup recommends that the certification program include a framework and processes for specifying and maintaining a current list of example technical standards that meet the base level of functionality specified in the standards for EHR certification.*

- EHR Modules: Certification of EHR modules that meet "at least one" certification criterion raises a number of security issues. A module that meets a security criterion but provides no health functions could be certified as an "EHR module" (e.g., an encryption module). Similarly, a module that meets an EHR criterion but neither provides nor calls any security services could be certified. If every module provides its own security services, security protection will be fragmented across the enterprise—but if only a subset of modules provide security services, there is no way to gain assurance that other modules will actually use (and not undermine) those services. *The Workgroup recommends making privacy and security criteria "addressable" for every EHR Module submitted for certification.*

- Audit: The audit-alerting criterion is beyond what is required by HIPAA or ARRA. Providing real-time audit alerting would require audit processing and decision support capabilities not available in most products today. Additionally, providing real-time alerting across multiple EHR modules would require a uniform data model, common vocabulary, and merge capabilities that are not available in currently available products. The standard indicates that audit data must be recorded when electronic health information is "created, modified, deleted or printed." Language in the IFR indicates that "access" should be audited; however, auditing of "printing" is difficult for small systems and would not include "print

screen." *The Workgroup recommends: (1) deleting the requirement for audit alerting; (2) adding "accessed" to the list of auditable actions; (3) replacing the term "printed" with "exported;" and (4) for 2013, consider adopting ASTM E2147 (Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems) as a standard for auditable actions and data elements that must be captured.*

- Integrity: There are concerns regarding the ambiguous scope of the integrity requirement in the IFR. *The Workgroup recommends clarifying the language to indicate that "detect alteration in transit" requires integrity verification only on the transmission channel and that the integrity of the message payload need not be independently verified.*

- Authentication: Although the certification criterion wording is somewhat ambiguous, the example of compliant standard cites IHE XUA profile with SAML assertions, which addresses sharing of user identity information between enterprises. XUA/SAML is not widely used within enterprises and very rarely between enterprises. The HITSC Standards Committee had recommended this for 2013, not for 2011. Although criteria and standards are specified for encrypting and integrity-protecting transmission channels, there is no criterion or standard for authenticating the end points of that channel. *The Workgroup recommends: (1) removing the certification criterion and standard for cross-enterprise authentication for reconsideration for 2013; (2) revising "cross-network" authentication certification criterion to read: "Verify that the identity of an entity seeking access to electronic health information across a network is the one claimed in accordance with the standard specified in §170.210(d);" and (3) revising standard §170.210(d) to read: "Authentication of the entities at each end of a protected transmission channel must be implemented."*

- Encryption Criterion: In the IFR, "user-defined preferences" could be interpreted as person-level proclivities instead of enterprise privacy and security policies. *The Workgroup recommends revising the "general" criterion to read "Encrypt and decrypt electronic health information according to entity-defined preferences in accordance with the standard specified in §170.210(a)(1)."*

- Encryption Standard: The IFR specifies a symmetric algorithm in functional terms, creating an opportunity to meet the requirement using a proprietary solution instead of the intended AES. Specifying "a symmetric…algorithm…must be used" precludes the use of public key (asymmetric) encryption. The preamble to the Breach Notification Rule cites FIPS 140-2 as a valid source of encryption processes, and FIPS 140-2 Annex A identifies three symmetric encryption algorithms (one of which is AES). *The Workgroup recommends revising the standard to read that: (1) for encryption and decryption of electronic health information, an algorithm recognized in FIPS 140-2, Annex A, must be used for symmetric encryption, or AES must be used for symmetric encryption; and (2) for exchange, the capability to establish a secure communication channel must be implemented.*

- Accounting of Disclosures: The 2011 criteria and standards appear to be out of sync with the timeline. The meaningful use objective for accounting of disclosure recommended by the HIT Policy Committee was targeted for 2015. For full accounting, with minimal adverse

impact to operations and system performance, there is a need to allow for generation of full accounting after the fact, rather than in real time. *The Workgroup recommends:*
  - *Postponing this certification criterion until 2013-2015.*
  - *Revising the certification criterion to read: "Create a record of disclosures made for treatment, payment, and health care operations…"*
  - *Revising the standard to read "(e) Create a record of treatment, payment, and health care operations disclosures. The date, time, patient identification, user identification, and a description of the disclosure must be included in the record of accounting of disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501."*
  - *Consider adopting data elements identified for "basic disclosure" accounting in ASTM E2147 as the standard.*

- Consumer Access: The meaning of "online access to their clinical information" is unclear, and language is inconsistent with meaningful use objective "Provide patients with timely electronic access to their health information..." "Online access" could be interpreted as "real-time" access and may not meet the HIPAA/ARRA requirement for "electronic copy." Additionally, it is unclear whether "electronic copy" should be human or machine interpretable, or possibly both, and it is not clear how to measure "meaningful usability" for the consumer. *The Workgroup recommends:*
  - *Revising to read: "Enable a user to provide consumers with electronic access to their health information, including, at a minimum, lab test results, problem list, medication list, medication allergy list, immunizations, and procedures, and to provide a copy of the consumer's personal health information in electronic format."*
  - *Establishing the specification of messaging and vocabulary standards for sending/transferring the electronic record to a PHR vendor as a priority for 2013.*
  - *Publishing guidance for developers and eligible professionals and hospitals on how to provide consumers timely electronic access to their health information.*

- Transport Standards: §170.202 adopts the Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) principles as standard protocols for electronically exchanging health information formatted in accordance with the standards adopted under §170.205. Although these protocols are commonly used, it is unclear what value including them in this IFR brings to the industry. These standards conflict with the section they reference, which requires HL7 messaging, NCPDP SCRIPT, and ASC X12N transactions. In addition, none of the certification criteria incorporate SOAP or REST directly or by reference to §170.202. *The Workgroup recommends removing §170.202 from the IFR.*

In addition to these concerns and recommendations, the Privacy and Security Workgroup noted some omissions and gaps in the IFR. For example, the IFR solicits feedback on the specific omission of DNS, LDAP, and consistent time. The Workgroup has no objection to this omission and suggests considering the addition of standards for time accuracy in 2013. Additionally, the omission of a certification criterion and standard for authenticating end points of a transmission channel between enterprises is a critical gap with respect to confidentiality, care quality, and patient safety. Finally, the omission of example standards in the body of regulation may be

perceived as a gap in the IFR; the Workgroup suggests that the ONC address the perpetual need for example current standards in planning for the certification program.

In discussion, the following points were made.

- In response to a question, Dixie Baker explained that in terms of the transport layer, the standards change fairly quickly, which is one of the reasons the Workgroup did not want to include the security-specific standards in the IFR.

- Wes Rishel supported the Workgroup's recommendation relative to §170.202, commenting that specifying neither the use of SOAP or REST by themselves is a statement that is sufficiently specific to assure that the level of confidentiality and endpoint authentication that is required. It would send a message that REST has not been ruled out, but it would indicate that anything that qualifies by the constantly evolving definition of what REST is would not automatically be accepted as meeting the requirements.

- A Committee member voiced strong support for a recommendation from the Workgroup to call out AES as an encryption standard. AES, it is a strong standard, widely available, and it is an American standard.

- Carol Diamond noted that if security is viewed as an attribute of tools that is enforced through certification as opposed to an attribute of practices and processes, it leads to added complexity without much additional protection. Dixie Baker explained that the certification certifies that encryption is in place, it does not certify that an organization is using it. The attributes of when something is encrypted is a policy decision, not a certification decision. There is a new workgroup of the HIT Policy Committee (the Privacy and Security Policy Workgroup) tackling these issues.

- With regard to EHR modules, Carol Diamond expressed concern about not taking into account the set of policies and practices needed to protect data inside and outside an organization. When data move outside an organization, there are security requirements that potentially can be looked at in the context of tools, but there is a much beiger requirement in terms of how they are used and how they are implemented. Dixie Baker commented that for this reason, the Workgroup agreed on "addressable" approach noted in the recommendation. If a module is supposed to do an internal calculation then the "addressability" is that the module does an internal calculation so the organization would not have to be concerned with authentication of users or with generating an audit record because of this internal calculation. Carol Diamond added that it would be helpful to clarify this point in the recommendation, specifically addressing what "addressable" means and does not mean.

- Carol Diamond noted that the requirement to provide electronic access may mean that the provider not only has to create the portal where the consumer can access information but also support and maintain this system. This may not be realistic for every data holder—simply allowing for download capabilities may be a reasonable work-around. Other services or applications that the consumer may choose to use can be utilized with that downloaded electronic copy. This would remove the burden of the provider having to be the application

provider for the consumer. Dixie Baker noted that the Workgroup's recommendations are consistent with this concept.

- In response to a question, Dixie Baker commented that there is a fundamental law in security such that the lower the level at which security is implemented, the harder it is to bypass, and the higher it is implemented, the finer the granularity of control. TLS and IPsec are intended for entirely different purposes. IPsec operates at the network level; TLS is at the transport layer, applicable for a finer granularity of control. Both are needed, and there should not be a recommendation to use just one or the other. Carol Diamond noted that IPsec does not work with many of the network address translation services widely used today.

- A Committee member noted that whatever the set of integrity protections are, they should specifically apply to data transfer by devices and media as well as messaging and electronic document and health information exchange. Support was voiced for the addition of a digital signature requirement for stage 1. Digital signature is a well-established standard that is widely used; it would provide important protections for consumers and providers and would be a reasonable addition to the stage 1 requirements.

- Chris Ross noted that the term "electronic access" can be problematic in that an unreasonable interpretation (but an interpretation nonetheless) of "electronic access" could be a month's worth of data dumped to a thumb drive. This represents electronic access, technically, but clearly is not what was intended in the IFR. There is no publicly specified shared view of what a PHR export format should look like. Revising IFR language to include "electronic access" has the potential to result in a lower level of capability to be technically compliant, but not helpful.

- Janet Corrigan noted that throughout many of the recommendations there are references to the security and privacy arrangements that pertain to the exchange of information between enterprises or between entities. The Committee is going to have to address the issue of what defines an enterprise or entity. Furthermore, it is anticipated that there will be tremendous innovation with regard to the development of new organizational structures. Some of these may have far less ability to protect patient identification, and they will differ tremendously in their capabilities internally.

- One Committee member suggested that in terms of administrative transactions within a modular system, there is a significant omission in need of clarification—what happens when clinical data is submitted with a claim, for example when there is an administrative event but also a disease management imperative and biometric data is being provided to a company as part of a commercial transaction? In addition, the term EHR has still not been sufficiently defined.

- David McCallie discussed the Workgroup's efforts related to the encryption standard and asked, given concern that encryption will be broken, how the highest possible standard for encryption can be regulated without naming it. Jodi Daniel explained that in drafting the IFR, the concern was that a specific standard would be locked in that then could get broken, resulting in vendors having to comply with a standard that the industry has moved beyond.

For this reason, functional standards, rather than specific standards, are being considered that would allow industries to develop more effective encryption approaches than what is included in the IFR.

- It was noted that there will be a certification body that will have to be recognized and will continue to have to prove itself capable of certification. This certification body may have some of the discretion Committee members have been seeking, especially when a criterion specifies a functional outcome rather than a specific standard.

- Jodi Daniel noted that with regard to the Workgroup's audit-related concerns and recommendations, the IFR does not specify that the alerts have to be automatic and discusses provider alerts based on user-defined events. The Workgroup's recommendation mentions providing real-time automatic audit alerting, which appears to be disconnected with what appears in the IFR. Dixie Baker commented that audit alerting is, by definition, near real time. The term "alert" also implies near real time in the context of an audit and in the context of an EHR.

- Jodi Daniel also mentioned that, relative to accounting for disclosure, the statute requires compliance for covered entities by January 1, 2011, for those who adopt after 2009, unless the Secretary modifies this compliance date. There is a concern that waiting until 2013 or 2015 would result in problems associated with the timing in the statute for complying with the accounting requirement and the standard. Dixie Baker suggested that this comment be passed along to the HIT Policy Committee, which has identified this as a 2015 meaningful use measure.

- Jodi Daniel asked about the authentication of entities at each end of a protected transmission channel. If there is a standard focused on authenticating at end points, how would that be addressed through a certification process that is certifying EHR technology? Dixie baker explained that it would come down to determining whether TLS or IPsec is supported, because both of those standards authenticate one or both ends of a transmission before establishing an encrypted channel.

- Carol Diamond explained that certified tools may encrypt data or offer the capability to have an audit log, but it is the processes and practices within an organization that determine whether or not information is protected. Most of the breaches that have taken place in the health care system have been within-organization events (e.g., stolen hardware, inappropriate look-up of celebrities, etc.); it would be ineffective to try to address them through tools or the capabilities of tools.

- In response to a question about accounting and disclosures, Dixie Baker suggested that the HIT Policy Committee receive a recommendation to identify a set of possibilities or data elements to create a minimal requirement. The meaningful use measure for accounting for disclosures is set for 2015 at present, and if Committee members think it should be sooner, that recommendation needs to be made to the HIT Policy Committee.

- Jonathan Perlin commented on the need to keep in mind HIPAA and that, regardless of what is specified as standard, there still exists the requirement with all appropriate penalties enforced to ensure that the protection of data. The standards are simply meant to specify tools.

- Cita Furlani noted that FIPS 140-2 is being revised and suggested that an encryption standard (whether it is FIPS, AES, etc.) should be specified in the Workgroup's recommendations.

- It was noted that although outside the scope of the Privacy and Security Workgroup, newborn screening and the transmission of that information greatly impacts the health care system. This information is the first meaningful record that is included in an individual's EHR. The IFR should include some type of vocabulary guidelines for newborn screening. With regard to the NPRM, there is going to be a need to evaluate newborn screening as an early part of the health record.

- Kevin Hutchinson suggested that, although it may fall outside the purview of the HITSC, some consideration be given to deterrents in the context of privacy and security (e.g., some level of deterrent or type of support around legislation making it illegal to hack into someone's EHR).

- John Halamka explained that the comments made during the discussion would be used to revise the Workgroup's letter to the HITSC Chair and Co-Chair.

> **Action Item #4:** Committee members accepted the recommendations of the Privacy and Security Workgroup by consensus, with the understanding that the letter to be submitted to David Blumenthal will be revised based on Committee discussion.

7. Implementation Workgroup: Update on Activities

The Implementation Workgroup will be holding an Implementation Starter Kit Hearing, to be held March 8, 2010, in Washington, DC. Liz Johnson explained that the Implementation Workgroup has put together four panels for the hearing: a public sector panel, two panels on implementation on experiences, and an innovation panel. She provided brief examples of the topics to be discussed during each of the panels. Any input related to the hearing can be submitted to the Workgroup online through http://healthit.hhs.gov/blog/faca/.

8. Public Comment

Deborah Peel of Patient Privacy Rights commented that her organization played a significant role in forming many of the IFR sections discussed at this meeting. The group worked with Congress on breach notice, accounting of disclosures, audit trails, encryption, and other topics. She voiced a criticism that members of the public are unable to read documents before Committee meetings and cannot provide comments during the meetings before the Committee takes a vote. She explained that in terms of breach notification, the intent of Congress is that there be a way to distinguish internal breaches from accidental access, and those that are not

accidental do need to be reported. In terms of audit trails, she expressed disappointment that any consideration is being given to pushing back developing meaningful audit trails and access to them to 2015. In terms of encryption, she explained that Congress never intended there to be a lock-down standard to be encryption. The language of the statute relates to the information being unreadable and undecipherable, because Congress did anticipate that encryption would be broken. The public wants audit trails soon, and wants them to indicate who accessed the record, for what purpose, and what portions were seen. Consumers currently do not have the right to control who sees their information electronically. Deborah Peel also noted that patients are entitled to their entire health record, not to some form of their record. She agreed with the Committee that it may be too confusing or too much information for some patients, but they have a right to it. John Halamka clarified that there was no recommendation of a delay with regard to audit by the HITSC or any of its workgroups. The NPRM itself has 2015 as the requirement for disclosure log.

Hans Buitendijk of Siemens Medical Solutions Health Services and a member of the HL7 Board of Directors noted codifying the version of a standard and/or implementation guide through federal rulemaking increases the risk of locking into older versions for too long that should and could reasonably be replaced by more current versions. He voiced support for the suggestion that rules include a minimum base standard floor to help address this challenge. He also commented that base standards allow for substantial optionality because they have to consider substantial variations in related use cases, whereas implementation guides can significantly reduce interpretation variations. To get to more widely used, consistent communication across health care providers, it would be helpful that through federal rulemaking a sanctioned structure be created with an open, consensus-based decision making process in which the industry stakeholders can come together to agree on most current implementation guidance, agree on reasonable take home target guidelines, where decisions are well documented and voted on, and with full opportunity for any stakeholder to participate and voice their perspective. He also commented that the suggestion to have the certification organization also write implementation guides incorporating appropriate source standard versions should not be considered good practice, particularly when multiple certifying organizations are in place.

Robin Raiford of Eclypsis commented that without a specific glidepath, industry does not have adequate time to test in their environment. Such direction and an adequate timeframe are needed to allow vendors to, for example, are building new pieces and translation tables within a database (months of advance notice, as opposed to weeks, are necessary).

SUMMARY OF ACTION ITEMS

Action Item #1: Minutes from the last HITSC meeting, held on January 20, 2010, were approved by consensus.

Action Item #2: The report of the Clinical Operations Workgroup was accepted by consensus.

Action Item #3: The Committee accepted the recommendations of the Clinical Quality Workgroup by consensus.

Action Item #4: Committee members accepted the recommendations of the Privacy and Security Workgroup by consensus, with the understanding that the letter to be submitted to David Blumenthal will be revised based on Committee discussion.